PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 10 October 2000 (10.10.00)	
International application No. PCT/DE00/00752	**Applicant's or agent's file reference** T99004 PCT
International filing date (day/month/year) 13 March 2000 (13.03.00)	**Priority date** (day/month/year) 12 March 1999 (12.03.99)
Applicant BRUNE, Peter et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

01 September 2000 (01.09.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Henrik Nyberg

Telephone No.: (41-22) 338.83.38

09/936420

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

To:

RIEBLING, Peter
Postfach 3160
D-88113 Lindau (Bodensee)
ALLEMAGNE

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

Date of mailing (day/month/year) 01 octobre 2001 (01.10.01)	
Applicant's or agent's file reference T99004 PCT	**IMPORTANT NOTIFICATION**
International application No. PCT/DE00/00752	**International filing date** (day/month/year) 13 mars 2000 (13.03.00)

1. The following indications appeared on record concerning:

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address	State of Nationality	State of Residence
DETEMOBIL Deutsche Telekom MobilNet GmbH Patentabteilung Landgrabenweg 151 53227 Bonn Germany		
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address	State of Nationality	State of Residence
RIEBLING, Peter Postfach 3160 D-88113 Lindau (Bodensee) Germany		
	Telephone No. 49-8382-78025/9692-0	
	Facsimile No. 49-8382-7 80 27	
	Teleprinter No.	

3. Further observations, if necessary:
Please note the newly-named agent in box 2. All further correspondence should be sent to this address.

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☒ the International Preliminary Examining Authority
☐ the designated Offices concerned
☒ the elected Offices concerned
☒ other: DETEMOBIL-former correspondence addr

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Dorothée MÜLHAUSEN
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

09/936420

D

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

SOLO 09/936420

REC'D 10 AUG 2001

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts T99004 PCT	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
Internationales Aktenzeichen PCT/DE00/00752	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 13/03/2000	Prioritätsdatum *(Tag/Monat/Tag)* 12/03/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04Q7/38		
Anmelder DETEMOBIL et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 4 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 4 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
01/09/2000	08.08.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter von der Straten, G Tel. Nr. +49 89 2399 8994

Formblatt PCT/IPEA/409 (Deckblatt) (Januar 1994)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/00752

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1,3-7	ursprüngliche Fassung			
2,2a	eingegangen am	25/05/2001	mit Schreiben vom	22/05/2001

Patentansprüche, Nr.:

1-8	eingegangen am	25/05/2001	mit Schreiben vom	22/05/2001

Zeichnungen, Blätter:

1/1	ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

1. Es wird auf das folgende Dokument verwiesen:

   D1 = DE, A, 197 18 103

2. **Betreffend Punkt V**

a. Der **Anspruch 1** betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer digitaler Mobilfunknetze. Solche Verfahren sind im Prinzip bekannt und zwar insbesondere aus der Druckschrift D1, die als Stand der Technik bezüglich Anspruch 1 angesehen wird.

   Dokument D1 offenbart in Übereinstimmung mit dem Oberbegriff des Anspruchs 1 ein Verfahren zur Verteilung von Schlüsseln an beispielsweise Teilnehmer digitaler Mobilfunknetze. Bei dem Verfahren der D1 gibt der Benutzer zum Zwecke seiner Autorisierung zusammen mit seiner Kennung eine Aufforderung zur Auswahl eines Schlüssels ein. Dieser Schlüssel wird dann vom Autorisierungsrechner ausgewählt und an den Benutzer gesendet. Der Benutzer verwendet diesen Schlüssel unmittelbar im weiteren Verlauf des Autorisierungsverfahrens.

   Das Verfahren gemäß Anspruch 1 unterscheidet sich von dem aus D1 in bekannten Verfahren durch den kennzeichnenden Teil.

   Ein solches Verfahren, bei dem ein Schlüssel einem Teilnehmer zugeordnet und im Endgerät des Teilnehmers abgespeichert wird, ist aus den im Recherchenbericht genannten Dokumenten nicht zu entnehmen und wird durch sie auch nicht nahegelegt. Dieses Verfahren hat den Vorteil, daß der Teilnehmer mehrere Schlüssel speichern kann, die er dann bei Bedarf verwendet.

   Der Gegenstand des **Anspruchs 1** ist folglich als neu und erfinderisch anzusehen, Artikel 33 (2) (3) PCT. Der Gegenstand des Anspruchs 1 ist ebenfalls gewerblich anwendbar.

b. Die abhängigen **Ansprüche 2 bis 8** beinhalten vorteilhafte Weiterbildungen des Gegenstandes des Anspruchs 1 und erfüllen somit ebenfalls die an sie zu stellenden Anforderungen bezüglich Neuheit, erfinderischer Tätigkeit und gewerblicher Anwendbarkeit.

Die DE-A-197 18 103 offenbart ein Verfahren zur Authentisierung in Datenübertragungssystemen, bei dem auf Anfrage eines Teilnehmers ein Schlüssel in Form einer Transaktionsnummer (TAN) von einem im Datenübertragungssystem vorgesehenen Authentisierungsrechner generiert oder aus einer Datei ausgewählt wird. Der Schlüssel wird von dem Authentisierungsrechner an den Teilnehmer übermittelt und kann dort vom Teilnehmer direkt zur Authentifikation gegenüber dem Authentifikationsrechner verwendet werden. Die Verteilung von mehreren Schlüsseln, die vom Teilnehmer je nach Bedarf verwendet werden können, ist aus diesem Dokument nicht zu entnehmen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäß wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kern der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation bzw. das Endgerät des Teilnehmers übertragen wird, wobei der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät und/oder einem Teilnehmeridentitätsmodul (SIM) der Mobilstation zur weitern Verwendung abgespeichert wird.

Das beschriebene Verfahren ist insbesondere geeignet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichern. Mit diesen Schlüsseln

kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdiensteknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Verteilung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

Patentansprüche

1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer digitaler Mobilfunknetze (7), wobei die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung (9) generiert und gegebenenfalls gespeichert werden und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung (9) angefordert und über das Mobilfunknetz (7) an eine Mobilstation (3) oder ein Endgerät (4) des Teilnehmers übertragen wird, dadurch gekennzeichnet,
dass der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät (4) und/oder einem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) abgespeichert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
dass auf dem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) eine SAT-Applikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung des zwischen Mobilstation (3) und Sicherheitseinrichtung (9) übertragenen Schlüssels vornimmt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet,
dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber dem Teilnehmeridentitätsmodul SIM (5) durch Eingabe einer PIN identifizieren muss.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet,
dass der übertragene Schlüssel auf einem geschützten Speicherbereich des Teilnehmeridentitätsmoduls SIM (5) abgespeichert wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet,
dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes (7) erfolgt.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes (7) in Form einer Kurznachricht SM erfolgt.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass bei Anforderung des Schlüssel die Berechtigung des Teilnehmers durch Auswertung einer Mobilteilnehmer-Rufnummer MSISDN des Teilnehmers geprüft wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (9) den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdiensteknoten (11) sendet.

If, furthermore, the added value service node is accessed via networks that are not secure, such as the Internet, there is a risk of the user name and password being monitored without authorization, and being misused.

The object of the invention is to specify a method using which keys can be distributed automatically to communications network subscribers using secure means.

According to the invention, this object is achieved by the characterizing features of the independent patent claim.

The essence of the invention is that the keys are generated, and may be stored if required, in a security device provided at the mobile radio network end, and in that on request by a subscriber, a key is requested from the security device, is allocated to the subscriber, and is transmitted via the mobile radio network to the subscriber's mobile station.

The described method is particularly suitable for distributing keys automatically to mobile terminals by secure means in a GSM or UMTS network, and for storing them on the subscriber's (U)SIM. A terminal user can use these keys to authenticate himself to an added value service node. The (U)SIM provides a protected-access medium in order to check passwords or keys, to store them and, when required, to use them for authentication, from a mobile radio network.

Patent Claims

1. A method for distributing keys to subscribers in communications networks, in particular digital mobile radio networks, characterized
in that the keys are generated, and may be stored if required, in a security device provided at the mobile radio network end, and in that on request by a subscriber, at least one key is requested from the security device, is allocated to the subscriber, and is transmitted via the mobile radio network to the subscriber's mobile station/terminal.

2. The method as claimed in claim 1, characterized
in that an SAT application is set up on the mobile station's SIM, and carries out additional end-to-end encryption of the information transmitted between the mobile station and the security device.

3. The method as claimed in claim 1 or 2, characterized
in that, in order to use the SAT application, the subscriber must identify himself to the U(SIM) by entering a PIN.

4. The method as claimed in one of claims 1 to 3, characterized
in that the transmitted key is stored in the terminal and/or in the mobile station's subscriber identity module U(SIM).

5. The method as claimed in one of claims 1 to 4, characterized
in that the transmitted key is stored in a protected memory area in the U(SIM).

6. The method as claimed in one of claims 1 to 5, characterized
in that the key is transmitted via a traffic channel in the mobile radio network.

7. The method as claimed in one of claims 1 to 5, characterized
in that the key is transmitted in the form of a short message (SM) via a signaling channel in the mobile radio network.

8. The method as claimed in one of claims 1 to 7, characterized
in that, when the key is requested, the subscriber's authorization is checked by evaluating the mobile subscriber telephone number MSISDN.

9. The method as claimed in one of claims 1 to 8, characterized
in that the security device sends the key which is transmitted to the subscriber to one or more added value service nodes.

1. FIGURE

2. Added value service node

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts T99004 PCT	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/DE 00/ 00752	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 13/03/2000	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 12/03/1999
Anmelder DETEMOBIL et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 00/00752

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04Q7/38 G07F7/10 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04Q G07F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 197 18 103 A (SCHMITZ KIM) 4. Juni 1998 (1998-06-04) das ganze Dokument	1,4,6-9
A	"GSM TECHNICAL SPECIFICATION GSM 11.14 VERSION 5.7.0" EUROPEAN TELECOMMUNICATION STANDARD,XX,XX, 1. April 1998 (1998-04-01), Seite COMPLETE66 XP002089350 Seite 12 -Seite 13	2,3

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12. Juli 2000	24/07/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Leouffre, M

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 00/00752

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19718103 A	04-06-1998	AU 6354598 A	05-11-1998
		CN 1207533 A	10-02-1999
		EP 0875871 A	04-11-1998
		JP 10341224 A	22-12-1998
		US 6078908 A	20-06-2000

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :
H04Q 7/38, G07F 7/10, H04L 29/06

A1

(11) Internationale Veröffentlichungsnummer: **WO 00/56101**

(43) Internationales Veröffentlichungsdatum: 21. September 2000 (21.09.00)

(21) Internationales Aktenzeichen: PCT/DE00/00752

(22) Internationales Anmeldedatum: 13. März 2000 (13.03.00)

(30) Prioritätsdaten:
199 11 221.5 12. März 1999 (12.03.99) US

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Deutsche Telekom MobilNet GmbH, Landgrabenweg 151, D–53227 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: BRUNE, Peter [DE/DE]; Noldestrasse 56, D–53340 Meckenheim (DE). SASSE, Andreas [DE/DE]; Zur Mühle 13, D–53773 Hennef (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS OF COMMUNICATIONS NETWORKS

(54) Bezeichnung: VERFAHREN ZUR VERTEILUNG VON SCHLÜSSELN AN TEILNEHMER VON KOMMUNIKATIONSNETZEN

(57) Abstract

The invention relates to a method of distributing keys to subscribers of communications networks, especially of digital mobile radio networks. Said keys are required, for example, for accessing value–added services. The aim of the invention is to provide a method for distributing said keys to the subscribers safely and above all in an uncomplicated manner. To this end, the keys are generated and optionally saved in a safety device provided at the end of the mobile radio network. Upon request of a subscriber, at least one key is requested from said safety device, is allocated to the subscriber and is transmitted to the mobile station of the subscriber via the mobile radio network.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Verteilung von Schlisseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen. Diese Schlüssel werden z.B. für den Zugang zu Mehrwertdiensten benötigt. Hierbei besteht das Problem, die Schlüssel sicher und vor allem unkompliziert an die Teilnehmer zu verteilen. Erfindungsgemäss wird dies dadurch erreicht, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen

Die Erfindung betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen, nach dem Oberbegriff des unabhängigen Patentanspruchs. Mit diesen Schlüsseln kann sich der Nutzer eines Endgeräts z.B. gegenüber einem Mehrwertdiensteknoten des Kommunikationsnetzes authentisieren.

Heute authentisiert sich ein Teilnehmer von Telekommunikationsdiensten beim Zugang zu Mehrwertdiensteknoten wie z. B. einer Mobilbox, durch Eingabe eines Paßworts und Nutzernamens. In GSM-Mobilfunknetzen wird dabei meist durch die Signalisierung die Mobilteilnehmer-Rufnummer (MSISDN) als Nutzername übertragen, womit eine explizite Angabe durch den Nutzer entfällt.

Die Vergabe und Nutzung des Paßworts (hier gleichbedeutend mit Schlüssel) ist ein kritischer Vorgang, da durch unerwünschte Offenlegung oder bewußtes Ausspähen dem Nutzer erheblicher Schaden durch Mißbrauch zugefügt werden kann. Neue Paßwörter werden daher häufig per Einschreibebrief versandt, was organisatorisch und technisch einen erheblichen Aufwand bedeutet und zugleich einen Zeitverzug, bis ein Paßwort beim Nutzer eintrifft.

Geschieht darüber hinaus der Zugang zum Mehrwertdiensteknoten über unsichere Netze wie z. B. das Internet, besteht die Gefahr, daß Nutzername und Paßwort unberechtigterweise abgehört und mißbraucht werden.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäss wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kern der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.

Das beschriebene Verfahren ist insbesondere geeignet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichern. Mit diesen Schlüsseln kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdiensteknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Verteilung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

Der berechtigte Nutzer der (U)SIM kann die Möglichkeit nutzen, den Schlüssel in andere Endgeräte zu transferieren bzw. mit dem mobilen oder anderen Endgeräten über Internet, PSTN oder ISDN auf die Mehrwertdiensteknoten zuzugreifen. Das Authentikationsverfahren zwischen Endgerät und Mehrwertdiensteknoten sowie der Transfer eines Schlüssels vom mobilen Endgerät auf ein anderes kann mit bestehenden Algorithmen gelöst werden und ist nicht Gegenstand der Erfindung.

In einer ersten Ausführungsvariante der Erfindung ist vorgesehen, dass der Nutzer einen neuen Schlüssel bei Bedarf durch eine Kurznachricht (SMS) abruft. Dazu sendet er eine Kurznachricht mit bestimmten Inhalt an eine durch den Netzbetreiber vorgegebene Zieladresse, die einer Sicherheitseinrichtung zugeordnet ist. Als Antwort erhält er von dieser Adresse ein Paßwort im Klartext zurück. Mit diesem Paßwort kann sich der Nutzer nun gegenüber einem Mehrwertdiensteknoten authentisieren.

In einer zweiten Ausführungsvariante der Erfindung, die ein höheres Sicherheitsniveau aufweist, ist vorgesehen, dass durch die Verwendung eines Programms auf der (U)SIM (Kartenapplikation), welches als Client mit dem Mobilfunknetz kommuniziert, alle Kommunikationsvorgänge zwischen Mobilstation und Sicherheitseinrichtung mit einem Ende-zu-Ende Verschlüsselungsverfahren verschlüsselt werden. In vorteilhafter Weise kann das Programm dem Nutzer eine menügeführte Oberfläche auf dem mobilen Endgerät bieten, mit der Schlüssel abgerufen und verwaltet werden können.

Zur Anforderung eines Schlüssels wählt der Nutzer z.B. einen entsprechenden Menüpunkt auf seinem Endgerät. Das Mobilfunknetz antwortet mit einer verschlüsselten Nachricht, die direkt an die Kartenapplikation gerichtet ist. Die Kartenapplikation speichert den Schlüssel in einem geschützten Speicherbereich der (U)SIM ab.

Zur Authentisierung gegenüber einem Mehrwertdiensteknoten wählt der Nutzer nach Eingabe einer PIN z.B. einen entsprechenden Menüpunkt an. Je nach Authentisierungsalgorithmus ist vorgesehen, dass

- der Schlüssel entweder im Klartext angezeigt und kann vom Nutzer weiterverwendet werden kann;
- der Schlüssel direkt zum Mehrwertdiensteknoten übertragen wird;
- der Schlüssel zu einem anderen Endgerät transferiert und dort weiterverwendet werden kann.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Im folgenden wird die Erfindung anhand eines Beispiels unter Bezugnahme auf eine Zeichnungsfigur näher beschrieben. Aus dem Beispiel, der Zeichnung und ihrer Beschreibung gehen weitere Merkmale und Vorteile der Erfindung hervor

Figur 1 zeigt eine Darstellung der beteiligten Systeme zur Durchführung des Verfahrens.

Die Mobilstation 3, welche ein Endgerät 4 umfasst, beherbergt in bekannter Weise die (U)SIM 5, auf der die Schlüssel zur Nutzerauthentikation gespeichert werden. Die Sicherheitseinrichtung umfasst einen Sicherheits-Server 9, der die Schlüssel nach einem vom Betreiber gewählten Algorithmus erzeugt, in einer Datenbank 10 speichert und die Schlüssel auf Anforderung 1 eines Teilnehmers an die (U)SIM 5 und die vom Teilnehmer nutzbaren Mehrwertdiensteknoten 11 verteilt.

Das Short Message Service Center 8 des Mobilfunknetzes 7 übermittelt die Schlüssel in Form von Kurznachrichten (SM) 2 zwischen Sicherheits-Server 9 und Mobilstation 3. Dies ist hier nur beispielhaft angegeben. Als Übermittlungseinrichtungen können z. B. auch GPRS-Knoten verwendet werden.

Gemäss einer ersten beim erfindungsgemässen Verfahren angewandten Sicherheitsstufe fordert der Teilnehmer einen Schlüssel über seine Mobilstation 3 durch eine Kurznachricht 1 an.

Der Sicherheits-Server 9 wertet die Anforderung aus, indem die Absendeadresse (MSISDN) des Teilnehmers auf Berechtigung geprüft wird, und sendet den oder die Schlüssel in einer Kurznachricht 2 an die Mobilstation 3, wo sie auf der (U)SIM 5 gespeichert wird. Darüber hinaus sendet der Sicherheits-Server 9 den Schlüssel an einen oder mehrere Mehrwertdiensteknoten 11. Die Schlüsselverteilung ist damit beendet. Der Nutzer kann sich nun je nach gewähltem Endgerät 4 und Zugangsweg (Mobilfunk, ISDN, Internet, etc.) gegenüber dem Mehrwertdiensteknoten 11 authentisieren.

Bei dieser niedrigen ersten Sicherheitsstufe basiert die Sicherheit der Schlüsselverteilung auf der Abhörsicherheit des GSM-/UMTS-Netzes und der Nutzeridentifikation per MSISDN. Einmal auf der (U)SIM gespeichert sind die Schlüssel über die Standard-PIN geschützt.

Bei der zweiten, erhöhten Sicherheitsstufe kann das SIM Application Toolkit (SAT) nach GSM 11.14 eingesetzt werden. Dazu wird eine SAT-Applikation auf die (U)SIM 5 eingebracht, die in dieser Client-Server-Konfiguration mit dem Sicherheits-Server 9 über das GSM- oder UMTS-Netz 7 kommuniziert.

Der Nutzer fordert Schlüssel über sein Endgerät 4 menüunterstützt über die SAT-Applikation an. Dazu muß er sich gegenüber der (U)SIM 5 mit einer zweiten PIN identifizieren, die er z.B. über die Tastatur des Endgeräts 4 eingibt. Danach versendet die SAT-Applikation eine verschlüsselte Anforderung 1 an den Sicherheits-Server 9, der die Anforderung verarbeitet. Der Sicherheits-Server 9 prüft die verschlüsselte Anforderung auf Echtheit anhand der Verschlüsselung sowie der Absendeadresse (MSISDN).

Bei positiv ausgefallener Prüfung erzeugt der Sicherheits-Server 9 den oder die Schlüssel für den Nutzer und sendet sie an die SAT-Applikation der (U)SIM 5 zurück. Die SAT-Applikation nimmt die Schlüssel entgegen und speichert sie in einem besonders geschützten Bereich der (U)SIM 5 ab. Darüber hinaus sendet der

Sicherheits-Server 9 den Schlüssel an einen oder mehrere Mehrwertdiensteknoten 11.

Der Zugriff auf die Schlüssel ist wiederum menügesteuert nach Eingabe einer PIN über die Kartenapplikation möglich, die einen ungebrauchten Schlüssel auf dem Display des Endgeräts 4 anzeigt oder auf Wunsch in einem ungeschützten SIM-Kartenspeicherbereich ablegt. Von dort kann dieser Schlüssel in einen PC/Laptop mittels Standard-Zugriffssoftware ausgelesen werden, z. B. mittels Chipkartenleser oder Infrarot-Schnittstelle des GSM-/UMTS-Endgeräts.

Alternativ und je nach Sicherheitsanforderung kann der Schlüssel auch vor dem Nutzer verborgen bleiben und vertraulich zwischen (U)SIM 5 und Mehrwertdiensteknoten 11 bzw. von der (U)SIM 5 zum Laptop/PC zwecks späterer Verwendung übertragen werden.

Ein besonderes Kennzeichen der zweiten Sicherheitsstufe ist eine zusätzliche Verschlüsselung der ausgetauschten Kurznachrichten 1, 2 zwischen dem Sicherheits-Server 9 (Server-SW) und der Software auf der (U)SIM 5 (Client-SW). Dadurch ist eine Ende-zu-Ende-Sicherheit zwischen Server-SW und Client-SW gegeben. Der Nutzer hat dabei vorzugsweise keine Kenntnis der dazu notwendigen Schlüssel. Als Verschlüsselungsalgorithmen zwischen Client und Server können Standardverfahren wie z. B. Triple-DES oder RSA zum Einsatz kommen.

Die für die Zusatzverschlüsselung notwendigen Schlüssel werden einmalig bei Personalisierung der (U)SIM eingebracht sowie auf den Sicherheits-Server geladen.

Zeichnungslegende

1	Signalfluss: Schlüssel anfordern
2	Signalfluss: Schlüssel laden
3	Mobilstation
4	Endgerät
5	(U)SIM
6	Luftschnittstelle
7	Mobilfunknetz
8	Kurznachrichtendienst-Zentrale
9	Sicherheitseinrichtung (Server)
10	Datenbank
11	Mehrwertdiensteknoten

Patentansprüche

1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen, dadurch gekennzeichnet,
dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und
dass auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation/ Endgerät des Teilnehmers übertragen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
dass auf der SIM der Mobilstation eine SAT-Applikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung der zwischen Mobilstation und Sicherheitseinrichtung übertragenen Informationen vornimmt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet,
dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber der (U)SIM durch Eingabe einer PIN identifizieren muss.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet,
dass der übertragene Schlüssel im Endgerät und/oder dem Teilnehmeridentitätsmodul U(SIM) der Mobilstation abgespeichert wird.

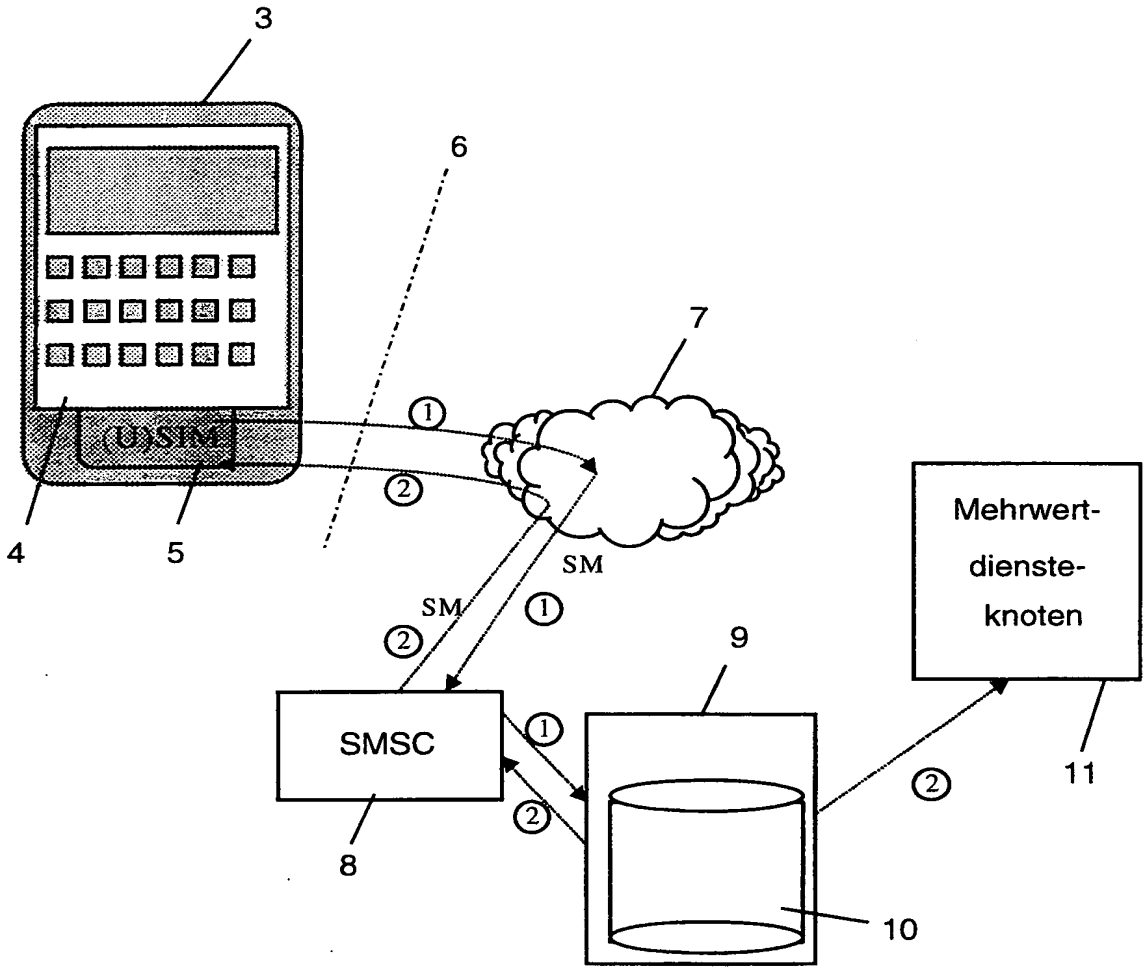
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet,
dass der übertragene Schlüssel auf einem geschützten Speicherbereich der U(SIM) abgespeichert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes erfolgt.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes in Form einer Kurznachricht (SM) erfolgt.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass bei Anforderung des Schlüssel die Berechtigung des Teilnehmers durch Auswertung der Mobilteilnehmer-Rufnummer MSISDN geprüft wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Sicherheitseinrichtung den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdiensteknoten sendet.


3
6
7
(U)SIM
1
2
4
5
SM
SM
1
2
9
Mehrwert-
dienste-
knoten
SMSC
1
2
2
11
8
10

FIGUR 1

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

BERICHTIGTE FASSUNG

9/936420

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. September 2000 (21.09.2000)

PCT

(10) Internationale Veröffentlichungsnummer
WO 00/56101 A1

(51) Internationale Patentklassifikation[7]: H04Q 7/38, G07F 7/10, H04L 29/06

(21) Internationales Aktenzeichen: PCT/DE00/00752

(22) Internationales Anmeldedatum:
13. März 2000 (13.03.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 11 221.5 12. März 1999 (12.03.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH** [DE/DE]; Deutsche Telekom MobilNet GmbH, Landgrabenweg 151, D-53227 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BRUNE, Peter** [DE/DE]; Noldestrasse 56, D-53340 Meckenheim (DE). **SASSE, Andreas** [DE/DE]; Zur Mühle 13, D-53773 Hennef (DE).

(74) Anwalt: **RIEBLING, Peter**; Postfach 3160, D-88113 Lindau (Bodensee) (DE).

(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

(48) Datum der Veröffentlichung dieser berichtigten Fassung: 30. Mai 2002

(15) Informationen zur Berichtigung:
siehe PCT Gazette Nr. 22/2002 vom 30. Mai 2002, Section II

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS OF COMMUNICATIONS NETWORKS

(54) Bezeichnung: VERFAHREN ZUR VERTEILUNG VON SCHLÜSSELN AN TEILNEHMER VON KOMMUNIKATIONSNETZEN

(57) Abstract: The invention relates to a method of distributing keys to subscribers of communications networks, especially of digital mobile radio networks. Said keys are required, for example, for accessing value-added services. The aim of the invention is to provide a method for distributing said keys to the subscribers safely and above all in an uncomplicated manner. To this end, the keys are generated and optionally saved in a safety device provided at the end of the mobile radio network. Upon request of a subscriber, at least one key is requested from said safety device, is allocated to the subscriber and is transmitted to the mobile station of the subscriber via the mobile radio network.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen. Diese Schlüssel werden z.B. für den Zugang zu Mehrwertdiensten benötigt. Hierbei besteht das Problem, die Schlüssel sicher und vor allem unkompliziert an die Teilnehmer zu verteilen. Erfindungsgemäss wird dies dadurch erreicht, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.

WO 00/56101 A1

Die DE-A-197 18 103 offenbart ein Verfahren zur Authentisierung in Datenübertragungssystemen, bei dem auf Anfrage eines Teilnehmers ein Schlüssel in Form einer Transaktionsnummer (TAN) von einem im Datenübertragungssystem vorgesehenen Authentisierungsrechner generiert oder aus einer Datei ausgewählt wird. Der Schlüssel wird von dem Authentisierungsrechner an den Teilnehmer übermittelt und kann dort vom Teilnehmer direkt zur Authentifikation gegenüber dem Authentifikationsrechner verwendet werden. Die Verteilung von mehreren Schlüsseln, die vom Teilnehmer je nach Bedarf verwendet werden können, ist aus diesem Dokument nicht zu entnehmen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäß wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kern der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation bzw. das Endgerät des Teilnehmers übertragen wird, wobei der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät und/oder einem Teilnehmeridentitätsmodul (SIM) der Mobilstation zur weitern Verwendung abgespeichert wird.

Das beschriebene Verfahren ist insbesondere geeignet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichern. Mit diesen Schlüsseln

kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdienstknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Verteilung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

Patentansprüche

1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer digitaler Mobilfunknetze (7), wobei die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung (9) generiert und gegebenenfalls gespeichert werden und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung (9) angefordert und über das Mobilfunknetz (7) an eine Mobilstation (3) oder ein Endgerät (4) des Teilnehmers übertragen wird, dadurch gekennzeichnet,
dass der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät (4) und/oder einem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) abgespeichert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
dass auf dem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) eine SAT-Applikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung des zwischen Mobilstation (3) und Sicherheitseinrichtung (9) übertragenen Schlüssels vornimmt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet,
dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber dem Teilnehmeridentitätsmodul SIM (5) durch Eingabe einer PIN identifizieren muss.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet,
dass der übertragene Schlüssel auf einem geschützten Speicherbereich des Teilnehmeridentitätsmoduls SIM (5) abgespeichert wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet,
dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes (7) erfolgt.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes (7) in Form einer Kurznachricht SM erfolgt.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass bei Anforderung des Schlüssel die Berechtigung des Teilnehmers durch Auswertung einer Mobilteilnehmer-Rufnummer MSISDN des Teilnehmers geprüft wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (9) den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdienstknoten (11) sendet.

INTERNATIONALER RECHERCHENBERICHT

Int. Aktenzeichen
PCT/DE 00/00752

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04Q7/38 G07F7/10 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04Q G07F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 197 18 103 A (SCHMITZ KIM) 4. Juni 1998 (1998-06-04) das ganze Dokument	1,4,6-9
A	"GSM TECHNICAL SPECIFICATION GSM 11.14 VERSION 5.7.0" EUROPEAN TELECOMMUNICATION STANDARD,XX,XX, 1. April 1998 (1998-04-01), Seite COMPLETE66 XP002089350 Seite 12 -Seite 13	2,3

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12. Juli 2000	24/07/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Leouffre, M

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int. ...ales Aktenzeichen
PCT/DE 00/00752

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19718103 A	04-06-1998	AU 6354598 A	05-11-1998
		CN 1207533 A	10-02-1999
		EP 0875871 A	04-11-1998
		JP 10341224 A	22-12-1998
		US 6078908 A	20-06-2000

INTERNATIONAL SEARCH REPORT

Int. tional Application No
PCT/DE 00/00752

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 G07F7/10 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 197 18 103 A (SCHMITZ KIM) 4 June 1998 (1998-06-04) the whole document	1,4,6-9
A	"GSM TECHNICAL SPECIFICATION GSM 11.14 VERSION 5.7.0" EUROPEAN TELECOMMUNICATION STANDARD,XX.XX. 1 April 1998 (1998-04 01), page COMPLETE66 XP002089350 page 12 -page 13	2,3

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 2000	24/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340 -3016	Leouffre, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/DE 00/00752

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19718103 A	04-06-1998	AU 6354598 A	05-11-1998
		CN 1207533 A	10-02-1999
		EP 0875871 A	04-11-1998
		JP 10341224 A	22-12-1998
		US 6078908 A	20-06-2000